REMARKS

The Office Action dated August 26, 2005 has been received and carefully noted. The following remarks are submitted as a full and complete response thereto. Claims 1-4, 7-17, 19-23 and 27-29 are currently pending in the application and are respectfully submitted for consideration.

In the Office Action, claims 1-4, 7-17, 19-23 and 27-29 were rejected under 35 U.S.C. §103(a) as being unpatentable over Tello (U.S. Patent No. 6,463,537) in view of Angelo (U.S. Patent No. 6,370,649). The Office Action took the position that Tello discloses all of the elements of the claims, with the exception of requesting a guess passcode from the manufacturer. The Official Action then relied upon Angelo as allegedly curing this deficiency in Tello. The above rejection is respectfully traversed for the reasons which follow.

Claim 1, upon which claims 2-4 and 7-12 are dependent, recites an apparatus for enabling functionality of a component. The apparatus includes an identification module having an identification number stored therein, a hash function module in communication with the identification module, a host in communication with the identification module, a guess register in communication with the host, an encryption module in communication with the guess register, and a public key module in communication with the encryption module wherein the public key module has a public key stored therein. The apparatus also includes a comparator in communication with the encryption module and the hash

function module, such that the comparator may compare a first bit string to a second bit string to generate a function enable output. The apparatus further includes a selecting device for selecting at least one of the function enable output and a bonding option output, the selecting device comprising an OR gate having at least one input for receiving said function enable output and the bonding option output. The host is also configured to communicate with a manufacturer to request a guess passcode corresponding to the identification number stored in the identification module.

Claim 13, upon which claims 14-17 and 19 are dependent, recites a component for selectively enabling functionality of an electronic device. The component includes a means for generating an encrypted bit string, a means for acquiring a guess passcode from a manufacturer, a hash function module in communication with an on board memory that has a predefined identification number stored therein, a means for determining if the encrypted bit string matches the guess passcode, and a means for outputting a functionality enable signal. The means for outputting includes a bonding option circuit, and an OR gate in communication with the bonding option circuit and the means for determining. The OR gate receives an input from at least one of the bonding option circuit and the means for determining and generates the functionality enable signal therefrom.

Claim 20, upon which claims 21-23 and 27-29 are dependent, recites a method for enabling functionality of an electronic component. The method includes the steps of encrypting a first bit string and a second bit string to generate a third bit string,

calculating a fourth bit string, comparing the fourth bit string to the third bit string, and generating a function enable signal in accordance with the comparison. The encrypting step further comprises the step of determining a guess passcode, which includes the step of requesting the guess passcode from a manufacturer. The method further includes the step of selecting at least one of a bonding option output and the function enable signal as a final enable output. The selecting step further comprises the steps of transmitting the bonding option output to an OR gate as a first input, transmitting the function enable signal to the OR gate as a second input, and generating the final enable output from the OR gate in accordance with the first and second inputs.

The prior art has failed to produce enablement methods that are effective against reasonably sophisticated attackers. The claimed invention resolves the limitations of the prior art by providing, in one example, a cryptographic method wherein the secure portions of the method are implemented in electronic or computer products. More specifically, embodiments of the claimed invention implement cryptographic functions for enabling functionality of electronic/computer related components, wherein the relevant secure key related information is contained within computer hardware in a non-volatile memory device and not within a purely software driven configuration. The claimed invention also provides the ability to conduct secure functionality enablement on electronic/computer related components, wherein a public key for enabling the component is contained onboard and utilized in conjunction with a randomly generated

component identifier in order to selectively enable additional functionality of the component.

As will be discussed below, the cited references of Tello and Angelo fail to disclose or suggest the elements of the claims, and therefore fail to provide the advantages and features discussed above.

Tello discloses a modified computer motherboard security and identification system. More specifically, Tello discloses a modified motherboard with a microprocessor based security engine, enabling and disabling circuits, memory buffer circuits, modified BIOS, modified DDL, and a smart card reader and smart cards. Upon startup of the computer, the modified BIOS takes control and allows the security engine microprocessor to look for and read from a smart card in the smart card reader that is connected to the security engine microprocessor. A unique hash number is placed in the smart card during the initial set up of the security system and a complimentary hash number is assigned to the security engine memory. During startup, a software program in the flash memory of the security engine compares the hash numbers in the smart card and the computer. If these two hash numbers are compliments, the boot up procedure is allowed to continue and access to the computer is allowed.

Angelo discloses a computer system with a self-modifying "fail-safe" password system that allows a manufacturer to securely supply a single-use password to users who lose or misplace a system password. The fail-safe password system utilizes a fail-safe counter, an encryption/decryption algorithm, a manufacturer's public key, and a secure

non-volatile memory space. Each time a fail-safe password is entered into the computer system, an application decrypts the fail-safe password and compares the resulting value, which is a hash code, to an internal hash value and increments the fail-safe counter or modifies the seed value when the hashes match. When the fail-safe counter is incremented, the previous fail-safe password is no longer valid.

Applicants respectfully submit that Tello and Angelo, whether considered alone or in combination, fail to disclose or suggest critical and non-obvious elements of the claimed invention. For example, both Tello and Angelo fail to disclose or suggest "a selecting device for selecting at least one of the function enable output and a bonding option output, said selecting device comprising an OR gate having at least one input for receiving said function enable output and the bonding option output," as recited in claim 1. In the Response to Arguments section, the Office Action alleges that this limitation of claim 1 is disclosed by Tello in Column 13, lines 15-17 and lines 56-67. Applicants respectfully disagree. Tello merely discloses two OR gates 305, 307 which each receive a control line (PIDEMST_CTRL and PIDESLV_CTRL) as one input and the output of FLIP FLOP 299 as the other input (see Figure 10A). When the control line is set to High, the primary I/O write, primary I/O read, and two PCS lines are disabled (Tello, Column 13, lines 58-64). Therefore, the enablement or disablement of the lines is completely dependent upon whether the control line is set to High or Low.

According to the present invention, on the other hand, cipher text generated by an encryption module 31 is compared to the guess passcode inserted into guess register 19

by host 18. If comparator 20 determines that the cipher text from the encryption module 31 matches the guess passcode, then an enable signal is sent from the output of comparator 20 to OR gate 23. OR gate 23 conducts a logical "OR" operation with inputs from comparator 20 and bonding option 25. Therefore, if either one of function enabler 32 or bonding option 25 indicates that the functionality is to be enabled, then an enable signal is transmitted from the output of OR gate 23 and is used to initiate the enabling of the desired functionality (Specification, Page 20, lines 10-20).

Applicants respectfully submit that the OR gates of Tello do not receive, as an input, a function enable signal or a bonding option output. Additionally, an enable signal is not transmitted from the output of the OR gate in Tello. Rather, the output of the OR gates is transmitted to AND gates (Tello, Figure 10A). Consequently, Applicants respectfully assert that the configuration of the circuit of the present invention (see Figures 2-4 of present application), as recited in claim 1, is not disclosed or suggested by that of Tello (see Tello, Figure 10A). Furthermore, Angelo also fails to disclose or suggest the elements of claim 1. As such, Applicants respectfully request that the rejection of claim 1 be withdrawn.

Similarly, Applicants respectfully submit that the combination of Tello and Angelo fails to disclose or suggest the means for outputting a functionality enable signal, as recited in claim 13. In particular, claim 13 recites that the means for outputting a functionality enable signal includes a bonding option circuit, and an OR gate in communication with the bonding option circuit and said means for determining. Further,

claim 13 recites that the OR gate receives an input from at least one of said bonding option circuit and said means for determining and generates the functionality enable signal therefrom.

As discussed above, with respect to claim 1, Applicants respectfully assert that both Tello and Angelo fail to disclose or suggest an OR gate which receives an input from at least one of the bonding option circuit and the means for determining and generates the functionality enable signal therefrom. As outlined above, Tello discloses the use of two OR gates receiving inputs from control lines and FLIP FLOP 299. The output of the OR gates are logically connected to AND gates 301, 303 (Tello, Figure 10A). Furthermore, Tello fails to disclose or suggest that the OR gates generate a functionality enable signal after receiving an input from at least one of the bonding option circuit and the means for determining. Angelo also fails to disclose or suggest such a limitation. Thus, the combination of Tello and Angelo fails to disclose or suggest all of the elements of claim 13.

With respect to claim 20, Applicants respectfully submit that Tello and Angelo, whether taken singly or combined, fail to disclose or suggest the step of selecting at least one of a bonding option output and the function enable signal as a final enable output. Claim 20 further recites that the selecting step also includes the steps of transmitting the bonding option output to an OR gate as a first input, transmitting the function enable signal to the OR gate as a second input, and generating the final enable output from the OR gate in accordance with the first and second inputs. As discussed above in reference

to claim 13, both Tello and Angelo fail to disclose or suggest an OR gate which receives the bonding option circuit as a first input and the function enable signal as a second input, and in turn generates the final enable output in accordance with the two inputs. Therefore, Applicants respectfully submit that the combination of Tello and Angelo fails to disclose or suggest all of the elements of claim 20.

Applicants note that claims 2-4, 7-12, 14-17, 19, 21-23 and 27-29 are dependent upon claims 1, 13, and 20, respectively. Therefore, claims 2-4, 7-12, 14-17, 19, 21-23 and 27-29 should be allowed for at least their dependence upon claims 1, 13, and 20, and for the specific limitations recited therein.

For at least the reasons discussed above, Applicants respectfully submit that the cited prior art fails to disclose or suggest critical and important elements of the claimed invention. These distinctions are more than sufficient to render the claimed invention unanticipated and unobvious. It is therefore respectfully requested that all of claims 1-4, 7-17, 19-23, and 27-29 be allowed, and this application passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the applicant's undersigned attorney at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the applicant respectfully petitions for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,

Majid S. AlBassam
Registration No. 54,749

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800
Fax: 703-720-7802

MSA:jf